App Privacy Labels
How Apple Exposes Data Collection Practices on the App Store

Jonas Vogel @ CocoaHeads Aachen - January 28, 2020

jonasvogel.name | iOS developer @ nextbike and RWTH i10 alumni
“Ask yourself:
Would you really want to live every day with that particularly annoying, privacy-invading advertisement profiling virtual agent that you are being asked to implement?”

— Prof. Dr. Jan Borchers, at the 2020 graduation speech @ RWTH Aachen
Outline

1. Basics
2. Examples
3. 3rd Party Dependencies & IDFA
4. Questions & Discussion
For each data type that your app collects, specify:

1. Why is it collected (e.g. App Functionality)?
2. Is it linked to the user?
3. Is it used to track the user?
“Tracking” refers to linking data collected from your app about a particular end-user [...] with Third-Party Data for targeted advertising [...] or sharing data collected from your app about a particular end-user or device with a data broker.

developer.apple.com/app-store/app-privacy-details/#user-tracking
Examples of App Privacy Labels

- Corona-Warn-App
- Spotify: Music and podcasts
- WhatsApp Messenger
- Signal - Private Messenger

Source: Signal App Store
You’re responsible for your dependencies!

• Google Firebase: informative discussion on GitHub which resulted in dedicated support article:
  • https://firebase.google.com/docs/ios/app-store-data-collection
  • https://github.com/firebase/firebase-ios-sdk/issues/5928

• Facebook Analytics: less transparency in data use. I personally consider anything sent there as “used for tracking”.

Related: Use of device’s advertising identifier (IDFA)

- Starting with iOS 14.5, Apple requires developers to ask permission to track
- New `AppTrackingTransparency` framework
- ID zeroed out if permission not granted
- Analytics SDKs tend to couple transmission of IDFA with linking of AdSupport framework

Source: Apple
Questions?

My prediction for August 2021

Following Cookie Hell - IDFA Consent Hell